AMENDMENTS TO THE CLAIMS

1-8. (Cancelled)

9. (New) A method for selecting a digital object in a database, the method comprising:

generating a plurality of encryption keys associated with a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the plurality of associated encryption keys to generate a plurality of digital object ciphertexts;

encrypting the plurality of encryption keys using a first key to generate a plurality of encryption key ciphertexts;

transmitting to a requester the digital object ciphertexts and encryption key ciphertexts;

receiving from the requester an encryption key ciphertext further encrypted using a second key;

decrypting the received encryption key ciphertext using the first key to generate a partially decrypted encryption key; and

transmitting the partially decrypted encryption key to the requester.

10. (New) The method of claim 9, further comprising encrypting the plurality of encryption keys by determining $(\text{encryption key})^{(\text{random number R})}$ mod (prime number p) for each key.

11. (New) The method of claim 9, further comprising decrypting the received encryption key ciphertext by determining $(\text{encryption key ciphertext})^{(1/(\text{random number R}) \bmod (\text{prime number p -1}))}$ mod (prime number p).

12. (New) The method of claim 10, further comprising performing the modulo operation if computation of a discrete logarithm is infeasible.

13. (New) A method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database a plurality of ciphertext digital objects;

receiving from the database a plurality of ciphertext keys associated with the plurality of ciphertext digital objects;

selecting a ciphertext key from the plurality of ciphertext keys;

further encrypting the selected ciphertext key using a first key to generate a further encrypted ciphertext key;

transmitting the further encrypted ciphertext key to the database;

receiving from the database a ciphertext key partially decrypted using a second key;

decrypting the partially decrypted ciphertext key using the first key to generate a decrypted key; and

decrypting the received ciphertext digital object using the decrypted key.

14. (New) The method of claim 13, further comprising encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

15. (New) The method of claim 13, further comprising decrypting the received encryption key ciphertext by determining (encryption key ciphertext)$^{(1/(\text{random number R}) \text{ mod } (\text{prime number p -1}))}$ mod (prime number p).

16. (New) The method of claim 14, further comprising performing the modulo operation if computation of a discrete logarithm is infeasible.

17. (New) A system for selecting a digital object in a database, the system comprising a processor for:

generating a plurality of encryption keys associated with a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the plurality of associated encryption keys to generate a plurality of digital object ciphertexts;

encrypting the plurality of encryption keys using a first key to generate a plurality of encryption key ciphertexts;

transmitting to a requester the digital object ciphertexts and encryption key ciphertexts;

receiving from the requester an encryption key ciphertext further encrypted using a second key;

decrypting the received encryption key ciphertext using the first key to generate a partially decrypted encryption key; and

transmitting the partially decrypted encryption key to the requester.

18. (New) The system of claim 17, wherein the processor is further configured or arranged for encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

19. (New) The system of claim 17, wherein the processor is further configured or arranged for decrypting the received encryption key ciphertext by determining (encryption key ciphertext)$^{(1/(\text{random number R}) \bmod (\text{prime number p -1}))}$ mod (prime number p).

20. (New) The system of claim 18, wherein the processor is further configured or arranged for performing the modulo operation if computation of a discrete logarithm is infeasible.

21. (New) A system for selecting a digital object in a database, the system comprising a processor for:

requesting a plurality of digital objects from an electronic database;

receiving from the database a plurality of ciphertext digital objects;

receiving from the database a plurality of ciphertext keys associated with the plurality of ciphertext digital objects;

selecting a ciphertext key from the plurality of ciphertext keys;

further encrypting the selected ciphertext key using a first key to generate a further encrypted ciphertext key;

transmitting the further encrypted ciphertext key to the database;

receiving from the database a ciphertext key partially decrypted using a second key;

decrypting the partially decrypted ciphertext key using the first key to generate a decrypted key; and

decrypting the received ciphertext digital object using the decrypted key.

22. (New) The system of claim 21, wherein the processor is further configured or arranged for encrypting the plurality of encryption keys by determining $(\text{encryption key})^{(\text{random number R})}$ mod (prime number p) for each key.

23. (New) The system of claim 21, wherein the processor is further configured or arranged for decrypting the received encryption key ciphertext by determining $(\text{encryption key ciphertext})^{(1/(\text{random number R})\ \text{mod}\ (\text{prime number p -1}))}$ mod (prime number p).

24. (New) The system of claim 22, wherein the processor is further configured or arranged for performing the modulo operation if computation of a discrete logarithm is infeasible.

25. (New) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

generating a plurality of encryption keys associated with a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the plurality of associated encryption keys to generate a plurality of digital object ciphertexts;

encrypting the plurality of encryption keys using a first key to generate a plurality of encryption key ciphertexts;

transmitting to a requester the digital object ciphertexts and encryption key ciphertexts;

receiving from the requester an encryption key ciphertext further encrypted using a second key;

decrypting the received encryption key ciphertext using the first key to generate a partially decrypted encryption key; and

transmitting the partially decrypted encryption key to the requester.

26. (New) The machine-readable medium of claim 25, wherein the method further comprises encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

27. (New) The machine-readable medium of claim 25, wherein the method further comprises decrypting the received encryption key ciphertext by determining (encryption key ciphertext)$^{(1/(\text{random number R}) \text{ mod } (\text{prime number p -1}))}$ mod (prime number p).

28. (New) The machine-readable medium of claim 26, wherein the modulo operation is performed if computation of a discrete logarithm is infeasible.

29. (New) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database a plurality of ciphertext digital objects;

receiving from the database a plurality of ciphertext keys associated with the plurality of ciphertext digital objects;

selecting a ciphertext key from the plurality of ciphertext keys;

further encrypting the selected ciphertext key using a first key to generate a further encrypted ciphertext key;

transmitting the further encrypted ciphertext key to the database;

receiving from the database a ciphertext key partially decrypted using a second key;

decrypting the partially decrypted ciphertext key using the first key to generate a decrypted key; and

decrypting the received ciphertext digital object using the decrypted key.

30. (New) The machine-readable medium of claim 29, wherein the method further comprises encrypting the plurality of encryption keys by determining $(\text{encryption key})^{(\text{random number R})}$ mod (prime number p) for each key.

31. (New) The machine-readable medium of claim 29, wherein the method further comprises decrypting the received encryption key ciphertext by determining $(\text{encryption key ciphertext})^{(1/(\text{random number R}) \bmod (\text{prime number p} -1))}$ mod (prime number p).

32. (New) The machine-readable medium of claim 27, wherein the method further comprises performing the modulo operation if computation of a discrete logarithm is infeasible.